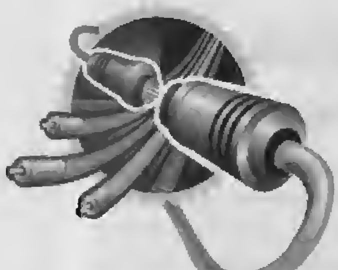
Ethernet Explained

Like other off-the-shelf technologies, Ethernet has become widely accepted in the world of automation. Understanding the basics is key to effective implementation.

Vance VanDoren
Control Engineering
and
Mario Bernardini
B&B Electronics



AT A GLANCE

- Origins of Ethernet
- Ethernet terminology
- Basic components
- Industrial applications

Ethernet was born in 1973 when Xerox's Bob Metcalfe sketched the basic concept on a napkin now archived at Xerox's Palo Alto Research Center. Originally designed for interoffice communications, Ethernet's performance and applications have expanded considerably in recent years.

The original standard operated at 2.94 Mbps (megabits per second). After Xerox partnered with Intel and Digital Equipment to develop the DIX 2.0 standard, Ethernet ran at 10 Mbps over thick coaxial cable. During the same time frame, the Institute of Electrical and Electronic Engineers (IEEE) started work on what is the current Ethernet standard known as CSMA/CD 802.3. In 1983, work by this group was finalized, and the standard was adopted.

More recently, Ethernet has migrated to the factory floor, where more than 100 protocols are available for exchanging data among a variety of industrial computing platforms—from intelligent sensors to plant-wide supervisory control systems. Ethernet owes its popularity in part to its longevity. It has been around for 30 years, it is the most common network protocol available, and engineers are familiar with it. It is a worldwide standard, software is abundant, and low-cost Ethernet products are widely available.

Ethernet also offers several technical advantages. It's fast and its extensive error correction mechanisms endow it with considerable robustness, even in harsh operating environments. It also offers reasonably good security through available encryption mechanisms.

Standards

So how does Ethernet manage to maximize the flow of data through a shared medium while keeping all the devices connected to the network from interrupting each other? It all depends on the IEEE standard for carrier sense, multiple access, and collision detection that regulates when and how data packets can be transmitted by one device and received by another.

Carrier sense describes the mechanism by which a device connected to the network checks to see if another device is already communicating. *Multiple access* means that all devices have access to the network to communicate as long as no other device is transmitting. *Collision detection* ensures that when multiple devices transmit simultaneously, the collisions are detected, and the corrupted Ethernet packets are discarded. The devices then wait different time intervals to retransmit.

But simply transmitting bits from one device to another is not enough to establish comprehensible communications. All that information must be organized in a hierarchical manner, much like letters must be organized into words, words into sentences, and sentences into paragraphs, to convey a written message.

Ethernet-based communication protocols generally do so according to the Open Systems Interconnect (OSI) reference model, sometimes called the "Seven-Layer Model" (see graphic). This model defines what a transmitting device must do to pack up a message for transmission and what the receiving device must do to unpack the transmission to recreate the original message.

This new connector interface for industrial Ethernet applications consists of the traditional RJ45 surrounded with other mechanical connections to seal it against the environment with an IP67 rating. Photo courtesy of B&B Electronics

Network Devices

The components common to most networks are hubs, switches, gateways, and routers. Ethernet allows only one sender and one receiver at each end of a cable segment. *Hubs* allow the network to branch and include more devices. Hubs are used to add devices, regenerate Ethernet packets, and extend network distances. Ethernet packets that are received by a hub are broadcast to all of its ports, simultaneously and indiscriminately.

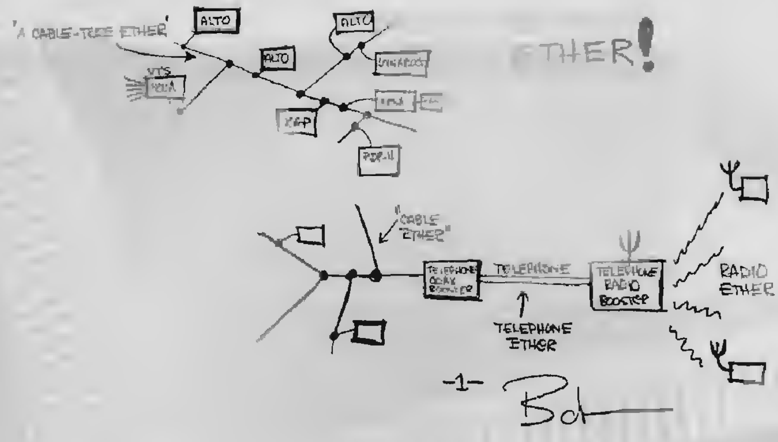
Switches filter and regenerate Ethernet packets to allow for greater network distances and more devices to be connected. Most switches segment the network at the data link layer into *collision domains* by sending data only to the desired destination.

Each switch has an addressing table listing the address of each connected device. When a packet is received, the switch stores and compares it to the address table, then forwards it to the correct port. This limits traffic on the other ports.

Managed switches were developed to give network managers control over network communications. Network traffic patterns are monitored and mirrored on a diagnostic port to troubleshoot problems and determine packet types. Each port can be enabled or disabled at half or full duplex, communication speed can be set, and flow control methods established.

A *gateway* is a device for interconnecting two or more dissimilar networks. It can translate all protocol levels from the physical layer up through the applications layer of the OSI model and can, therefore, interconnect entities that differ in all details.

Routers divide networks into subnets by filtering network traffic by IP address. When networks are logically instead of physically divided (as with switches), only IP addresses destined for appropriate devices can pass through. If a packet is going to the immediate segment, the packet will be forwarded. If it is destined for a different segment or router, it will be tagged with appropriate information and sent on. Routing occurs at the network layer.



The original idea for the Ethernet (c. 1973), drawn on a napkin by Bob Metcalfe, showed how data could be transmitted and received through a network of cables, phone lines, and radio signals, some of which would be shared by multiple devices. Source: Palo Alto Research Center

An additional benefit of a router is its ability to block broadcast and corrupted packets, which greatly reduces network traffic on subnets.

Industrial Ethernet

The Ethernet developed for industrial applications follows the same constructs as the commercial Ethernet used for interoffice communications, and it uses the same OSI model. However, the two differ in the robustness of the equipment used.

Light industrial Ethernet products are designed for environments harsher than the office. They feature mounting hardware to make components physically secure in standard industrial enclosures and wide-range power input options that eliminate costly wall-mount transformers. Redundant power sources add protection, and operating temperature ratings of 0-60 °C guard against premature failure.

Common certifications for light industrial Ethernet products include Class 1, Div. 2, shock, freefall, and vibration ratings. Testing for electromagnetic interference (EMI) and radio frequency interference (RFI) minimizes data corruption from welders and radios.

For heavy industrial environments, Ethernet products must be hardened and extremely rugged. In many cases they are installed outdoors or on the plant floor. They must be built to withstand power surges, ultra-wide temperature ranges of -40 °C to 80 °C, high humidity, unstable power sources, and exposure to chemicals and corrosive materials.

In these applications, explosive atmospheres, contact with liquids, and radiation also threaten

Seven layer model

Layer	Function	Network Hardware	Protocols
Application (Layer 7)	Provides service to user	Most gateways operate at this layer	Supports applications and user authentication; Provides services for e-mail, network software, telnet, FTP application; Contains actual information that the user wants to send
Presentation (Layer 6)	Translates data into the desired form to be displayed on PC; Translates between two different formats.		
Session (Layer 5)	Allows applications to communicate across the network	Gateway	NetBIOS
Transport (Layer 4)	End-to-end control of data once communication path is established		TCP, UDP, ARP, RARP
Network (Layer 3)	Routes messages, controls flow of data between devices	Routers, Layer 3 switches	IP, ARP; RARP, ICMP; RIP; OSFP, IGMP
Data link (Layer 2)	Establishes protocols or rules to send data across physical layer Logical link control Media access control	Ethernet switches, bridges, network interface cards	MAC address
Physical (Layer 1)	Cables, connectors, transmitters, receivers	Hubs	

ONLINE

For additional coverage search "Ethernet" at *Control Engineering* Online www.controleng.com

B&B Electronics offers two supplements to this article: "The Ethernet Buzzword Guide" and "Ethernet Basics Guide." The latter provides additional information on network design. To access these supplements, visit *www.bb-elec.com*.

the safety of equipment and people. This necessitates more constraints on enclosure design. High levels of EMI/RFI may require copper cage housing construction. The extreme levels of shock and vibration in heavy industrial settings require close attention to mechanical integrity and shock testing.

Cables

Whether in the office or on the plant floor, Ethernet uses a structured cabling system that supports a multi-product, multi-vendor environment. The EIA/TIA-568 standards for structured cabling developed by the Electronic Industries Alliance and Telecommunications Industries Association specify such details as the maximum allowable horizontal copper run (90 meters), maximum patch cord length (5 meters), and the minimum copper wire bend radius (four times the diameter of the cable).

Additional standards apply to networks that are to function in an industrial environment, including a new connector type currently being defined by the EIA/TIA. It contains at its core the familiar 8-pin modular plug and connector.

Vance VanDoren is consulting editor, Control Engineering, www.controleng.com; Mario Bernardini is product manager for wired Ethernet products, B&B Electronics, www.bb-elec.com.

Industrial Ethernet organizations include:
www.ethercat.org
www.ethernet-powerlink.org
www.fieldbus.org
www.iaona.org
www.modbus-ida.org
www.odva.org
www.profibus.org
www.sercos.org